

State of the Industry: Deploying Enterprise PKI

March 1999

Daniel Blum
Senior Vice President
Principal Consultant

The Burton Group
dblum@tbg.com
www.tbg.com

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Deploying Enterprise PKI

Agenda

- Level Set: PKI Status
- Issues, Myths, and Transition
- PKI Policy and Architecture Integration Points
- Recommendations

THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

What is PKI?

- PKI is the set of services that allow corporations to deploy and use public key security systems, including digital certificates
- Certificates bind a public key to an “owner”
 - Establishes identity (a person, a company)
 - Signed by a trusted party (chains of trust)

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

PKI Solves EC Business Problems

- Open new markets
- Authenticate trading partners to enforce business rules on electronic commerce
- Maintain privacy and integrity of secure email and electronic transactions
- Secure, controlled remote access anywhere/anytime by employees and associates

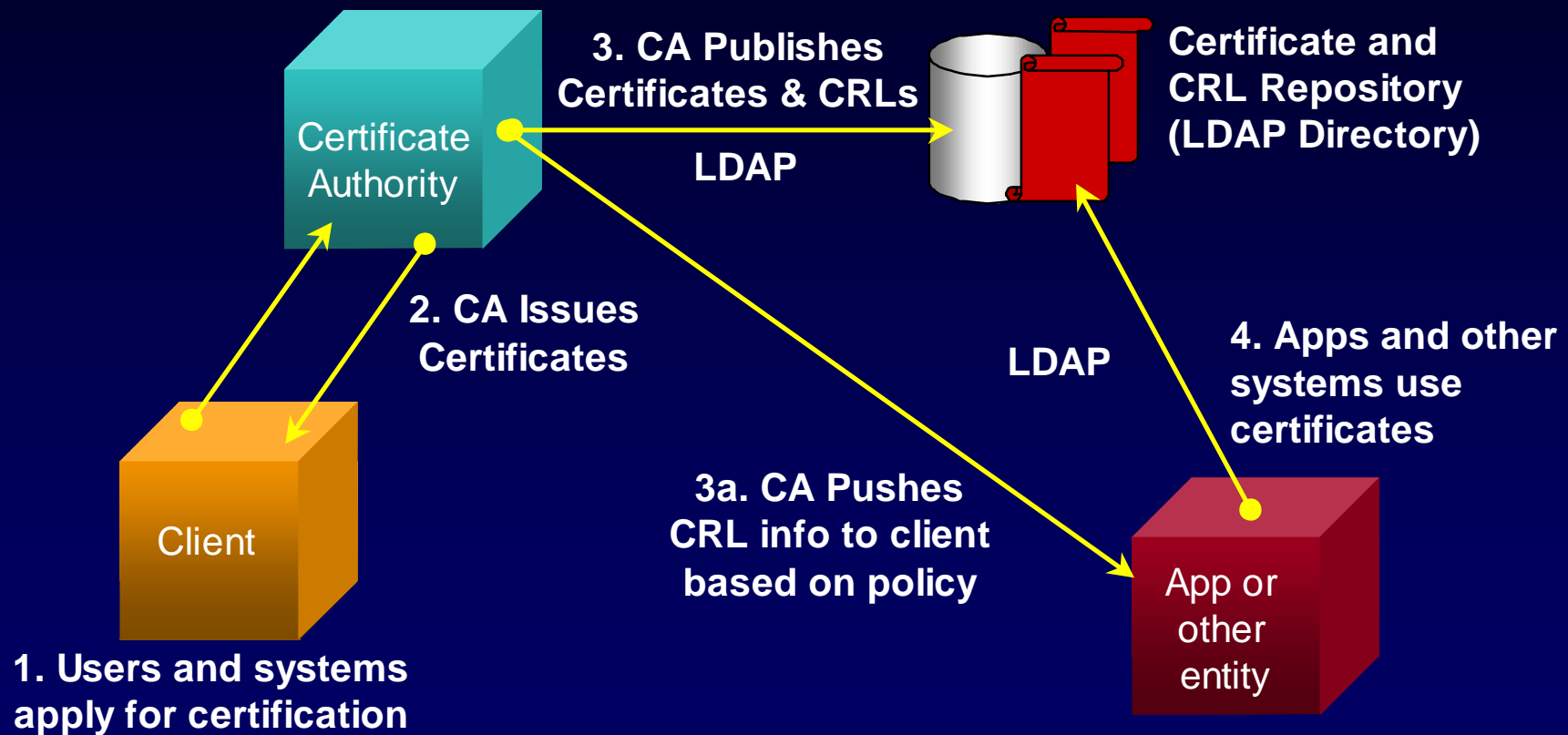
THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

Level Set: PKI Basics



THE BURTON GROUP

In-depth technology analysis for network planners

Deploying Enterprise PKI

Level Set: Other important PKI requirements

- Registration authorities
- Trust relationships
- Key backup/recovery
- Non-repudiation
- Archive/retrieval (key history)
- Time stamping

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

Agenda

- Level Set: PKI Status
- Issues, Myths, Transition
- PKI Policy and Architecture Integration Points
- Recommendations

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

PKI Issues

- Where is the Interoperability?
 - X.509 is very general, interoperability not guaranteed
 - The IETF PKIX committee moves slowly
 - Divergent approaches: Certificate management, requests, revocation, online verification, authorization
- How many lawyers does it take to change a PKI?
 - Will PKI play in Peoria? Maybe...
 - But international legal applicability is uncertain

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

Issues: The Mythical Single Certificate

- Enterprises would like to have a general purpose certificate
- Many applications require their own special purpose certificates
- You can't have a single certificate unless you also have a single private key, but portability is hard
- Even if every application could use the same certificate in theory, policy and trust divergences prevent it in practice

THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

However:

- Customers can't afford to wait
- Instead, they must

Enable Transition

THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

The transition...

Low assurance



Graduated assurance

Weak authentication



Smartcard, Biometric

Browser PKI



Managed PKI

Pair-wise interoperability



General interoperability

Special purpose CAs



General purpose CAs

THE BURTON GROUP

In-depth technology analysis for network planners

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

What are peer organizations doing?

- The typical organization is just getting started
- Evidence from surveys through our consulting division suggests perhaps 50% or more of Fortune 500 enterprises plan to deploy PKI in 1999
- This may mean pilots, or limited operational capabilities, not full production
- Lots of customers are holding off, describing their issues to us as:
 - ease of use, integration, liability, interoperability, manageability, scalability
- But there are many innovative applications today

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

PKI Products and Services

- Baltimore Technologies
- Entrust
- GTE Cybertrust
- IBM/Lotus
- Microsoft
- Netscape
- Novell
- Thawte
- Valicert
- Verisign
- Worldtalk
- Xcert

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

Agenda

- Level Set: PKI Status
- Issues, Myths, and Transition
- PKI Policy and Architecture Integration Points
- Recommendations

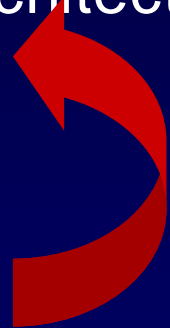
THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

Deployment Stages

- Take inventory
 - Perform Requirements Analysis
 - Develop PKI Policy
 - Identify Integrating Architecture and Strategy
 - Product Selection
 - Deployment
 - Integration
 - Life cycle management
- 

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

PKI Policies

- Certificate Policy (CP): Defines PKI rules for an application(s), an enterprise, or community. It governs the levels of:
 - Assurance
 - Identification and authentication
 - Liability limits
 - Security controls
 - Records management
 - Audits

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

PKI Policies

- Certificate Practice Statement (CPS)
 - Detailed statement of the operational procedures, standards and practices used by a CA in carrying out its functions under the CP.
- Different levels of assurance require different CPSs, or Certificate Policies

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

Understand PKI Architecture, Integration Points

- Applications and APIs
- CA trust relationships
- Directory Repositories
- PKI-using Application protocols
 - S/MIME
 - SSL
 - SET
- PKI Management Protocols (PKIX)
 - Certificate Management Protocol (CMP)
 - Public Key Cryptography Standards (PKCS)

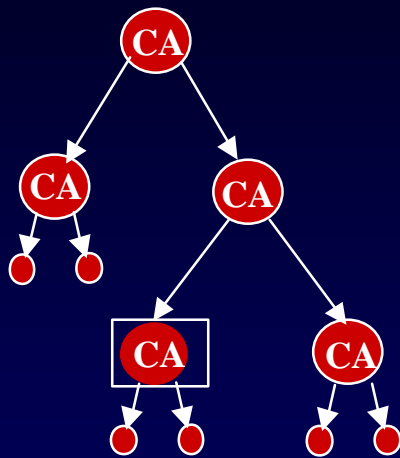
THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

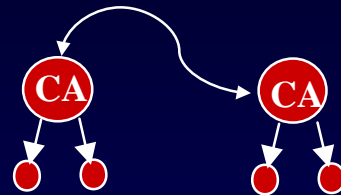
Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

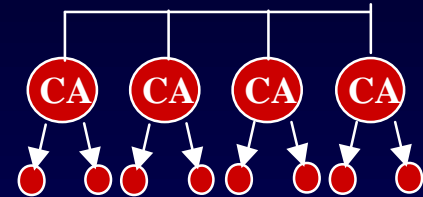
Extend EC Through Certificate Authority Trusts



Hierarchical trust
Uses Certification paths
Found in large enterprises



Meshed trust
Uses Cross Certificates
Used bilaterally



Certificate Trust List
Flat list of certs
Can apply to a client,
enterprise, or community

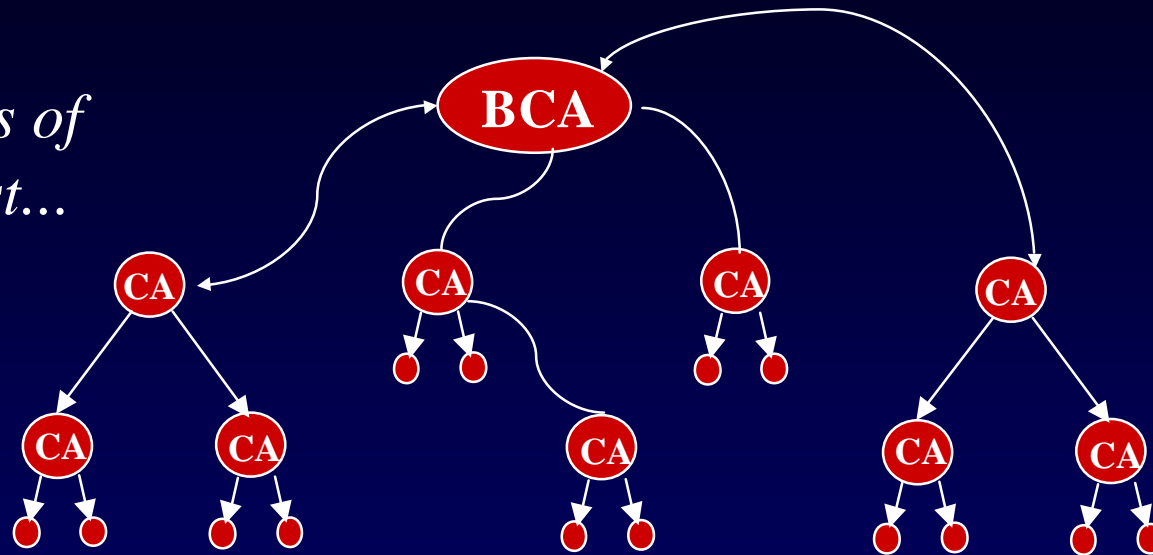
THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Deploying Enterprise PKI

Join Communities

Webs of Trust...



BCA: Bridge CA links together meshed CAs or hierarchically organized CAs. Can apply to communities, such as Federal PKI (FPKI), Automotive Network Exchange (ANX), Worldwide Insurance Networks (WINS), NACHA

THE BURTON GROUP

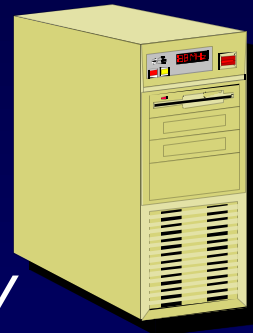
In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Deploying Enterprise PKI

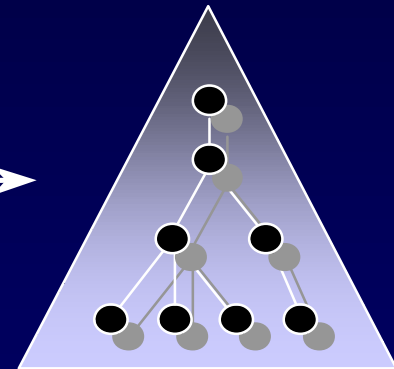
Integrate PKI with Directory Processes

- Determines naming
- Provides the repository
 - Certificates
 - CRLs
 - Policies
 - CA info
- Enables *manageability*

**Certificate
Authority
Service**



**Directory
Repository
Service**



THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Deploying Enterprise PKI

Agenda

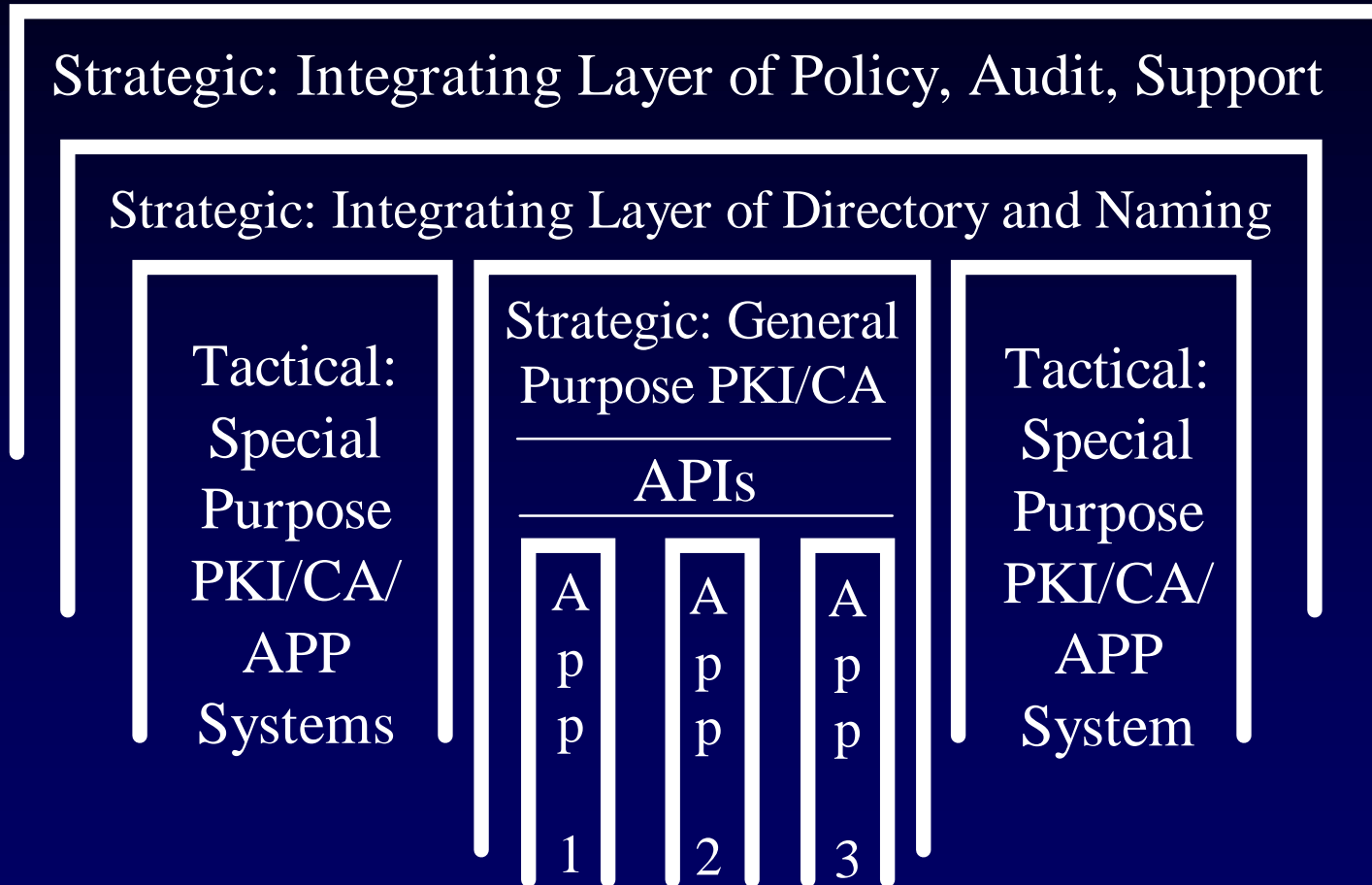
- Level Set: PKI Status
- Issues, Myths, and Transition
- PKI Policy and Architecture Integration Points
- Recommendations

THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

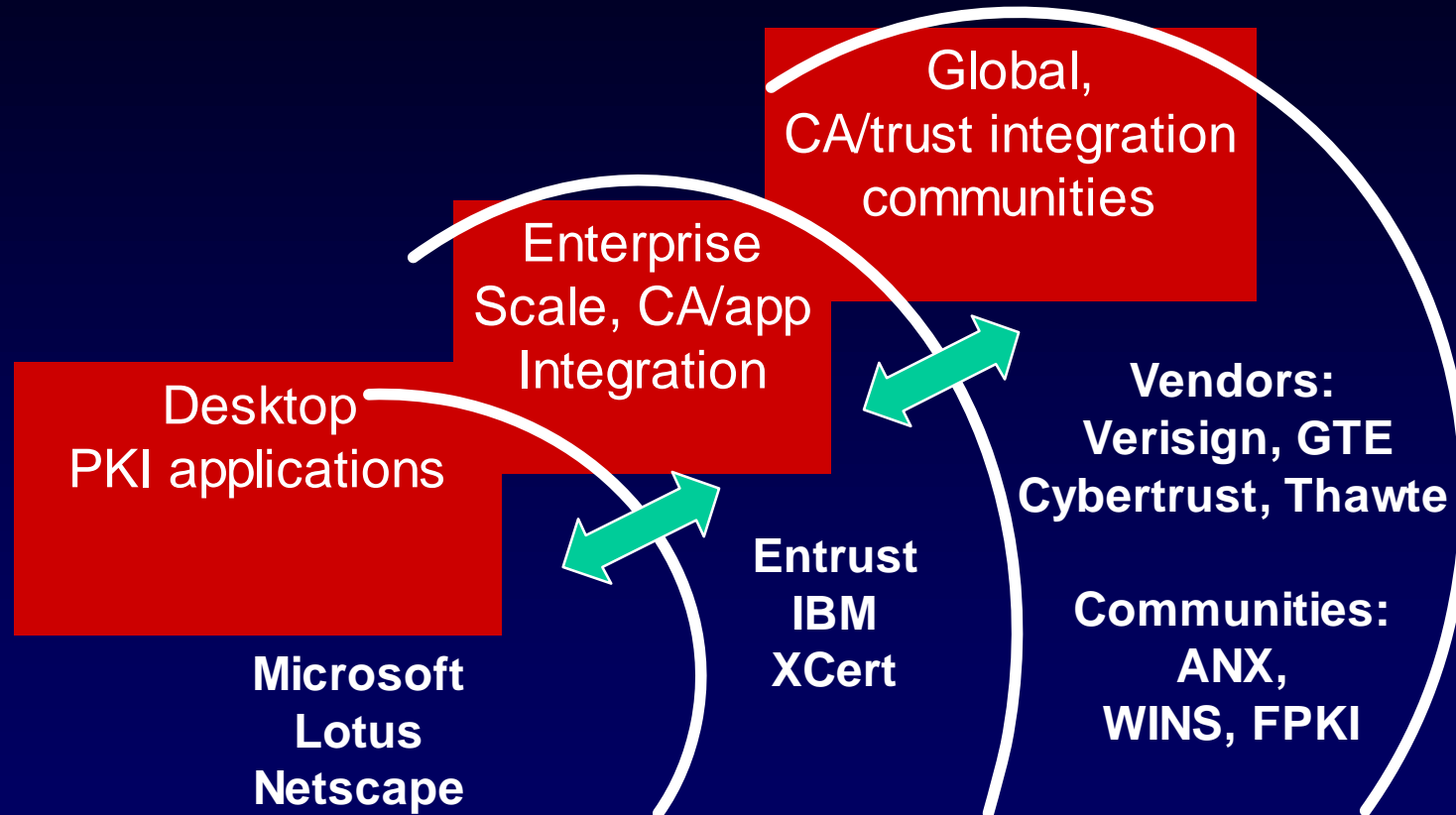


THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Deploying Enterprise PKI

Products / Architecture Levels



THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Deploying Enterprise PKI

Recommendations: Focus on manageability

- If it greatly increases the admin burden, PKI won't be deployable enterprise-wide
- Certificates will be usable when they can be managed like passwords
- Day-to-day user management should be directory enabled and integrated with PKI
 - Create a user, create a cert
 - Delete a user, revoke a cert
- Plan, design, train, automate, simplify, and integrate.

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

Relate Directory, PKI, and Management



THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Deploying Enterprise PKI

Thesis.

Stepping up to Manageable PKI enables the electronic commerce opportunity.

By the end of 1999, customers must have robust PKI policies, strategies, skill sets, and pilots in place.

THE BURTON GROUP

I n - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s

Copyright © 1999 The Burton Group All Rights Reserved.

Questions and Answers

THE BURTON GROUP

In - d e p t h t e c h n o l o g y a n a l y s i s f o r n e t w o r k p l a n n e r s